REMARKS/ARGUMENTS

Claims 1, 3, 5, 7, 8, 10-12, 19, 20, 22-24, 28-32, 34, 38-41, 48-50, 72, 73, 75-81, and 93 are pending in the application. Claims 1, 3, 5, 7, 8, 10-12, 19, 20, 22-24, 28-32, 34, 38-41, 48-50, 72, 73, 75-81, and 93 stand rejected as obvious under 35 U.S.C. § 103. The rejection is respectfully traversed and reconsideration is requested. The reference asserted does not teach or suggest the claimed invention.

Claim Amendments

The amendment of independent method claims 1, 32, 41, 81, and 93, and independent system claim 81 proposes that in addition to having a local aspect residing on the owner's terminal, a remote aspect residing on a trusted third party's server, a virtual execution function, and a virtual archivist function, the virtual wallet application is also configured at least in part for storing data representing at least one of a payment mechanism and electronic funds (See, e.g., p. 1, lines 21-23; p. 8, lines 20-29; and p. 9, lines 20-23) and that in addition to periodically updating the remote aspect with the data stored on the local aspect, the virtual archivist function also periodically reformats the data stored on the remote aspect of the virtual wallet application to conform to succeeding methods of accessing the stored data. See, e.g., p. 10, lines 20-24 and p. 11, lines 6-15.

Support for the foregoing amendment is found throughout the specification and in the claims as detailed above. Accordingly, no new matter has been added.

Claim Rejections - 35 U.S.C. § 103

Claims 1, 3, 5, 7, 8, 10-12, 19, 20, 22-24, 28-32, 34, 38-41, 48-50, 72, 73, 75-81, and 93 stand rejected under 35 U.S.C. § 103(a) as obvious over Carman et al. (U.S. 6,272,632).

Carman et al. disclose a method and system for recovering encrypted data when the secret key with which the data was encrypted is unavailable. There is

absolutely no suggestion, however, in Carman et al. of storing the data on a virtual wallet application with a local aspect residing on the owner's terminal, a remote aspect residing on a trusted third party's server, a virtual executor function, and that is also configured for storing data representing a payment mechanism and/or electronic funds, according to Applicants' claimed invention. On the contrary, Carman et al. teaches an encrypting system that encrypts data using a secret key and generates a key recovery field including the secret key that is in turn encrypted by a 'key recovery center' public key, the corresponding private key for which is stored in the 'key recovery center'. The public key is acquired and an access rule controlling access to the secret key is defined in a registration phase by an 'access rule defining system'. See, e.g. Carman et al., Col 2, lines 20-32 and Col 12, lines 41-45.

While it is true that the access rule of Carman et al. can include a method for releasing a will only after death has been independently verified, there is no teaching or suggestion in Carman et al. of automatically assigning a primary aspect of a secret access device for the virtual wallet application to the owner by the virtual wallet application for accessing the stored data and automatically escrowing a secondary aspect of the secret access device for the virtual wallet application by the virtual executor function conditioned on the occurrence of the event that renders the owner incapable of acting on the owner's own behalf, according to Applicants' claimed invention. Instead, the 'access rule defining system' of Carman et al. specifies the access rule and sends it to the 'key recovery center' which returns an access rule index to the 'access rule defining system' for use by the 'encrypting system' to create the key recovery field. Thus, when the secret key is lost, the 'key recovery center' uses the access rule index to locate the access rule with which to control a challenge to the 'emergency decrypting system' to determine its right to access. See, e.g. Carman et al., Col 7, line 58-Col 8, line 4.

Nor does Carman et al. teach or suggest periodically updating the remote aspect of the virtual wallet application with the data stored on the local aspect by the virtual archivist function of the virtual wallet application via the network and

periodically reformatting the data stored on the remote aspect of the virtual wallet application by the virtual archivist function to conform to succeeding methods of accessing the stored data, according to Applicants' claimed invention. On the contrary, FIG. 9 of Carman et al. and the accompanying text merely illustrates nothing more than the process of changing the access rule when the 'access rules defining system' desires or deems it necessary to change the definition of an existing access rule. See, e.g., Carman et al., Col 11, lines 45-63.

Neither does Carman et al. teach or suggest receiving verification of the occurrence of the event by the trusted third party from a personal representative of the owner upon the occurrence of the event and accessing the stored data by the trusted third party on behalf of the owner's personal representative with the escrowed secret access device, according to Applicants' claimed invention. Rather, when the secret key of Carmen et al. is lost, the 'emergency decrypting system' extracts the key recovery field from the document and sends it to the 'key recovery center' which responds with a challenge defined by the previously registered access rule. If the 'emergency decrypting system' successfully answers the challenge, the 'key recovery center' releases the secret key contained in the key recovery field to the 'emergency decrypting system' for use in decrypting the encrypted data. See, e.g., Carman et al., Col 6, lines 33-58.

Accordingly, Carman et al. do not disclose, nor even suggest, the required combination of limitations of independent claims 1, 32, 41, 81, and 93 of Applicant's claimed method and system for securely storing data for an owner. Because the cited reference does not teach the limitations of independent claims 1, 32, 41, 81, and 93, the Examiner has failed to establish the required *prima facie* case of unpatentability. See In re Royka, 490 F.2d 981, 985 (C.C.P.A., 1974) (holding that a *prima facie* case of obviousness requires the references to teach all of the limitations of the rejected claim); See also MPEP §2143.03. The Examiner has failed to establish the required *prima facie* case of unpatentability for independent claims 1, 32, 41, 81, and 93, and similarly has failed to establish a *prima facie* case of unpatentability for claims 3, 5, 7,

8, 10-12, 19, 20, 22-24, 28-31, 48-50, 72, 73, and 75-80 that depend on claim 1 and claims 34 and 38-40 that depend on claim 32, and which recite further specific elements that have no reasonable correspondence with the references.

Conclusion

In view of the foregoing amendment and these remarks, each of the claims remaining in the application is in condition for immediate allowance. Accordingly, the examiner is requested to reconsider and withdraw the rejection and to pass the application to issue. The examiner is respectfully invited to telephone the undersigned at (336) 607-7318 to discuss any questions relating to the application.

Respectfully submitted,

Date: 6/14/04

John M. Harrington (Reg. No. 25,592)
for George T. Marcou (Reg. No. 33,014)

Kilpatrick Stockton LLP
607 14th Street, NW, Suite 900
Washington, DC 20005
(202) 508-5800